PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A1

(11) International Publication Number: WO 99/26123

(43) International Publication Date: 27 May 1999 (27.05.99)

(21) International Application Number: PCT/GB98/03470

(22) International Filing Date: 18 November 1998 (18.11.98)

(30) Priority Data:

9724411.5	18 November 1997 (18.11.97)	GB
9804503.2	3 March 1998 (03.03.98)	GB

(81) Designated States: CN, JP, US, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

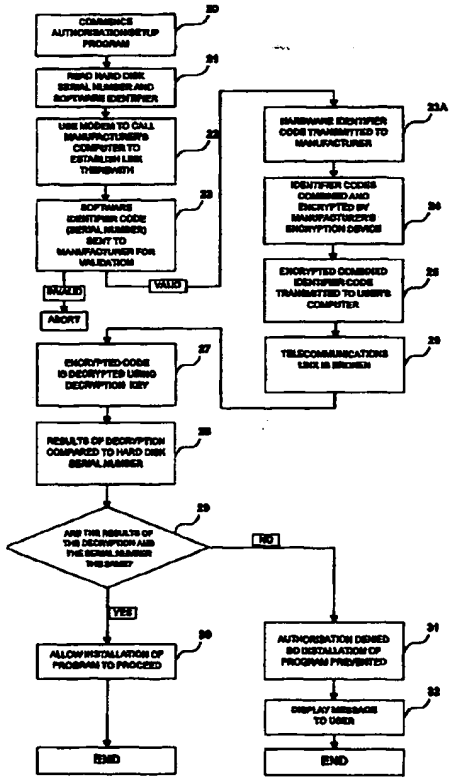
(71)(72) Applicant and Inventor: WAKELY, Christopher, Benjamin [GB/GB]; 19 Deards Wood, Knebworth, Hertfordshire SG3 6PG (GB).

(74) Agent: RUNECKLES, John, Frederick; Llewelyn Zietman Solicitors, Temple Bar House, 23–28 Fleet Street, London EC4Y 1AA (GB).

(54) Title: IMPROVEMENTS RELATING TO SOFTWARE PROTECTION SYSTEMS

(57) Abstract

A method and a system of preventing unauthorised installation or running of a program in a computer is described. The method includes reading (21) an identifier code associated with the computer which is preferably the hard disk serial number (7) and an identifier code associated with the program. This number (7) is sent (23, 34) to a third party (e.g. the software manufacturer) where they are combined and encrypted (25, 35) using a private encryption key (17). The encrypted data relating to the combined identifier codes is received at the computer and is decrypted (27) using a stored public decryption key (5). Installation of the program is prevented (31) if the computer identifier code (7) is not equivalent to or derivable from the decrypted data.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Improvements Relating to Software Protection Systems

Field of the Invention

The present invention concerns improvements relating to software protection systems and more particularly, though not exclusively, to a method of and a system for preventing unauthorised installation, copying and/or running of a program in a data store of a computer.

Background of the Invention

For many years now, one of the greatest problems facing the computer software industry has been how to protect against widespread illegal copying of its products. This problem costs the industry billions of dollars in lost sales and makes it considerably more difficult for the industry to recoup its investment in research and development of new products.

There have been several attempts to overcome this problem which have been unsuccessful as they have been easily circumvented by software pirates. For example, for software delivered on 3½ inch floppy disks, it is possible to write a disenabling code back to the disks during installation, thereby making it difficult to accomplish or actually preventing subsequent installations of the software program onto other computers.

In US Patent 4,748,561, for example, there is described a method in which the "disenabling code" is obtained from identification information unique to the

computer on which the software program is first run, this identification information being written back to the disk containing the software program during the initial running of the disk on the computer. The "written back" information is compared by means of a routine written into the software with the corresponding identification information of the computer on each occasion the software is subsequently run. In the event that the "written back" information is not identical to that of the computer then the program aborts and will not load. A similar method is employed in US patent 4,688,169. In both methods the unique machine identifier which is used to generate the disenabling code may be installed in machine readable form within a component of the computer hardware eg a PROM or as part of the computer's motherboard or may be located in an operating system or an applications program.

All the methods described above rely in part for their efficacy on the writing back of information onto the original medium on which the software programs are loaded. Unfortunately they are relatively easily circumvented by copying the original disks prior to the first installation or running and subsequently using these copies for each separate installation.

With software delivered on CD-ROM any writing to the disk is impossible, therefore an alternative arrangement has been used by some manufacturers. A CD key or serial number is provided on the back of the CD case. This key is input by the user during the installation process. Unfortunately

this arrangement does not prevent installation of the software on other computers, nor does it prevent the copying of the CD-ROM as long as the CD key or serial number is also copied at the same time. With the advent of relatively low-cost CD writers, the copying of CD-ROMs is likely to increase.

In another method devised to overcome the problem addressed by the present invention a serial number is hard coded into the software on the CD-ROM. When the software is installed a random key or serial number is generated and the user is asked to telephone the software manufacturer or supplier for a registration number. This registration number is then input by the user and the installation process completes. Unfortunately, because CD-ROMs are pressed in very large batches the hard coded serial numbers are common to a large number of CD's and because they are combined with randomly generated keys or serial numbers, it is impossible for a supplier to know if the registration numbers he supplies are for valid copies of his software. It is thus possible for a large number of pirate copies of the software to be installed by unsuspecting users without the supplier being aware. The software can also be easily copied illegally onto many machines. A further drawback of this method is that it has been discovered that replacing just one small data file turns unregistered software into registered software.

US Patent 5,337,357 describes a method of protecting software distributed in encrypted form from unauthorised use in which the authorisation to load and

use one or more of a number of independent or related programs supplied in combination with a multiplicity of other programs on a CD-ROM is obtained by the user transmitting to a remote location a unique identifier obtained from his computer hardware. In this method the unique identifier, which may came from a PROM installed by the hardware manufacturer or may be some other unique "fingerprint" of the computer, is accessed by an installation routine contained within the software. The identifier is used to generate a key which is transferred to a remote location (eg a central processing section). The remote location then encodes this key and retransmits the encoded key which is inserted into the computer by the program installer and which is used to unlock those of the encrypted programs for which authorisation is required. This method does not, and is not intended to, prevent the disk on which the encrypted programs are originally loaded being copied or used a large number of times.

Summary of the Invention

The present invention aims to provide an improved software protection method and system which addresses at least some of the above problems and provides greater security against illegal copying of software.

In its broadest aspect, the invention resides in the appreciation that none of the prior art methods described above relies upon a process of marking or tagging software as it is copied or installed in a computer with an identifier that is a combination of identification keys that are specific both to the software

program itself and to the computer hardware on which it is first installed or copied and that with such marking or tagging unauthorised installation or running of software could be made much more difficult and, in certain circumstances, prevented altogether.

According to a first aspect of the present invention there is provided a method for preventing unauthorised installation, copying or running of a computer program on a computer comprising the steps of reading an identifier code associated with the computer; combining and encrypting the computer identifier code with an identifier code associated with the program, tagging the computer program with the encrypted combined identifier codes as it is installed from its storage medium onto the computer or is copied via the computer onto another or recipient medium; decrypting the combined codes and comparing the decrypted tagged computer identifier code during running of the installed program, or during subsequent installation of the copied program, with the identifier code of the computer on which the program is installed or is being installed from the said recipient medium; and preventing the running of the program or its installation if the second computer identifier code is not identical to or derivable in a pre-determined manner from the tagged identifier code.

Preferably, the computer hardware identifier code with which the computer program is tagged or marked is obtained from the permanent data store (i.e. the hard disk) of the computer. The hard disk serial (or volume) number is

readily readable by a security installation program running either from a CD-ROM or other installation medium or from the hard disk of the computer and at run time by an installed application. The identifier code may also be, for example, derived from the configuration of the computer and its associated hardware (e.g. printer, modem, serial and parallel ports etc) or may be a serial number specifically coded into and associated with the CPU or a PROM forming part of or associated with the CPU which can be accessed via an installation program or the hard disk of the computer and also at run time.

The tagging or marking of the software program as it is loaded (or, if on a writeable medium, copied) may, for example, be performed by a routine written into the installation software itself which reads the identifier code of the computer and carries out the encryption and combination steps and then writes the resultant encrypted code into the program during installation. Alternatively the tagging may be achieved by a routine written into the operating system of the computer which automatically runs with any disk copying or installation routine of the operating system; or by a separately loaded security software program. During the first installation of the program from a writeable storage medium (e.g. a 3½" floppy) the tagging or marking of the software will normally take the form of tagging of both the program loaded on the computer and of the installation medium (to prevent its re-use on another computer).

The step of comparing the computer identifier code tagged into the

software program with the identifier code of the computer upon which the program is run, or is being installed from a disk which contains a tagged program, may also be performed by a routine loaded with the program or by a sub-routine of the computer's own operating system.

The steps of encryption and decryption increase the level of security provided by the method of the present invention because it might otherwise be possible to access the combined tagged identifier code within the software and change it to the machine identifier code of a second computer. The use of encryption makes it more difficult for a hacker or unauthorised user of the software who is able to access the tagged computer identifier codes to change them to that of his own computer.

Preferably the encryption/decryption is performed by use of private key/public key cryptography, more particularly by using an implementation of the RSA algorithm as described in more detail in, for example, "Data & Computer Security" by Dennis Longley and Michael Shain, Macmillian Reference Books. The usual method used in public/private key cryptography involves the use of an enciphering key which is in the public domain and a deciphering key which is kept secret. Using such cryptography anyone can encipher data using the public key of another user, but only those users with knowledge of the secret key can decipher enciphered data. The preferred method of the present invention reverses the normal usage of the keys and uses the secret key to encrypt the identifier code

and the public key to decrypt the identifier code. As the secret key is not available to the user it is not possible for him to generate independently the encrypted identifier code which is needed to enable the software to be installed and run on another computer. Such cryptography is particularly suitable because, as will be described later, it is possible to ensure that the hardware identifier code is encrypted with the private key remotely by the software supplier or manufacturer and can then only be decrypted using the public key contained within the program. The strength of public/private key cryptography is based on the fact that if the generating numbers chosen are sufficiently large it is computationally infeasible to calculate the private key given the public key and possibly other information, such as a modulus. Therefore it is not possible for the dishonest user to replace the encrypted hardware identifier code with that of his own computer.

Copying and modifying the installed program, so it will run on another computer, is made very difficult by use of public key/private key cryptography in association with the method of the present invention. However, in the embodiments described above the encryption key is contained in the software and it may be possible for a determined copier or hacker to extract it and to use it to break the protection. In order to overcome this disadvantage it is a particularly preferred method of the present invention to include in the software a routine that requires the further steps of transmitting the software and hardware identifier

codes to a remote location (e.g. that of the software manufacturer or the software supplier) for encryption with an encryption key and inputting this remotely encrypted identifier code to tag or mark the program.

There are various methods by which the hardware and software identifier codes can be transmitted to the software manufacturer or supplier or other remote location for encryption and the encrypted data can be re-transmitted and used to tag or mark the computer program which will be obvious to anyone skilled in the art. These include, without limitation, the user or installer of the program being notified of the hardware and software identifier codes on the computer screen during installation and communicating them to the manufacturer or supplier for encryption via a telephone network. The combined encrypted code is given back to the installer who inputs it into the computer to tag or mark the program as it is installed and, as described above, on the original storage medium if this is possible. The communication between the installer and the manufacturer or supplier may be by voice or by electronic means using, for example, the signals generated by a touch tone telephone.

In another embodiment, a modem link is established between the installer's computer and the software supplier's or manufacturer's computer via a telephone network preferably via the internet so that the encryption and tagging processes can be carried out automatically without user interaction. It is also possible to provide the encrypted data via other non-telephone wide area

networks.

When the program which is tagged with the encrypted hardware and software identifier codes is run, the decryption key will operate to verify that the program is being run on a computer with the same machine identifier code and will either enable the program to be run unhindered or will prevent it running and, for example, the user will be presented with a warning message regarding unauthorised use.

The transmission of the combined hardware and software identifier codes to the software manufacturer or supplier enables him to maintain a data base of registered software users which includes the specific information of each user's hardware identifier. This will enable the supplier or manufacturer to authorise (by, for example, re-transmitting to the user/installer an appropriate encrypted key) the subsequent re-installation of the original software, eg when necessitated by some fault with the originally loaded software or when a hardware fault necessitates reloading. It will also allow the supplier to authorise subsequent installation of the software onto another computer if he believes that there is a bona fide reason for such re-installation (eg upgrading of the computer hardware, hard disk replacement or re-formatting necessitated by hardware or software faults or viruses). Where the supplier is contacted by the same installer or by a second person using the identifier of an already registered hard disk or other hardware identifier he will be able effectively to prevent installation if he thinks

the re-use is not bona fide.

The method of the present invention will provide a much higher level of security even when the hard coded serial numbers of CD-ROMs (which are batch, rather than CD-ROM, specific) are used as the software identifier. However maximum security can be obtained with the method of the present invention when software supplied on CD-ROM, or other read only medium, is being installed by utilising a unique recognition label (serial number) provided with each legitimate copy of the CD-ROM (such as the product ID usually provided on the outside of a sealed envelope or plastic case of the CD-ROM as supplied by the manufacturer) as the software identifier that is transmitted to the software supplier or manufacturer for combination with the readable identifier code of the computer. The supplier or manufacturer then combines and encrypts both the software label ID and the hardware identifier and transmits back to the installer a combined access code. Installation and running of the program will only proceed if both the hardware code and the software label are equivalent to or derivable in a predetermined manner from decrypted data to enable installation of the program. Otherwise, the program is prevented from being installed or run and the user is notified of the refused authorisation.

The further step of transmitting both the software ID and the hardware identifier code to the software supplier/manufacturer provides the supplier/manufacturer with the possibility of maintaining a database linking the

identity of each registered user to his or her hardware and software. Attempts to register and use illegal copies of software will be effectively brought to the attention of the software manufacturer/supplier who will then be able to take appropriate protective measures.

This embodiment of the invention prevents copying and modifying the installed program so it will run on another computer. It also prevents illegal re-use of the installation medium, or a copy of the installation medium, on another computer, because it is possible for the software manufacturer or supplier to determine if any request for authorisation has been generated from a valid copy of the software. Any legal re-use of the installation medium, e.g. if the owner wishes to re-instal the software on his computer or on a replacement or upgraded hard disk or on a new computer purchased as a replacement can of course, be authorised by the manufacturer who will have visibility because the necessary authorisation procedure will need to be re-performed.

Although it is currently the practice for large batches of CD-ROMs to be pressed from a common master, in which case all the CD-ROMs of a batch are identical and any serial numbers contained within the software are also identical, CD-ROM blanks could be modified to include a small writeable section in which a unique recognition label could be written. With a CD-ROM containing such a unique recognition label the process of reading the label and combining it with the identifier code of the computer could be performed by the program itself.

According to another aspect of the present invention there is provided a security system for preventing unauthorised installation of a program in a computer or copying of a program by a computer, the system comprising: means for reading an identifier code of the computer; means for reading an identifier code of the program; means for combining and encrypting the two identifier codes; means for tagging the program with the combined encrypted identifier code during installation or copying; means for decrypting the encrypted codes and comparing the tagged computer identifier code with the identifier code of the computer on which the program is run or being installed from a copy; and means for preventing installation of said program if the tagged identifier code is not equivalent to or derivable from that of the computer on which the program is running.

When the identifier code of the computer is a serial number specifically coded into a PROM forming part of, or associated with, the CPU the method of the present invention has the added advantage of being capable of making it difficult for the CPU to be used by an unauthorised user (e.g. as a result of theft of the CPU). In order to instal a computer containing a stolen PROM-containing CPU with software which contains the encryption, decryption routines which form part of the present invention, the installer will need to register the software and hardware identifier codes with the software supplier/manufacturer and this will be identifiable from the records held by the supplier/manufacturer.

The invention also extends to a combination of a system as described above and an encryption apparatus provided at a location remote from that of the system, and arranged to encrypt the identifier codes using an encryption key.

The above and further features are set forth with particularity in the appended claims and together with the advantages thereof will become clearer from consideration of the following detailed description of several exemplary embodiments of the prevent invention given with reference to the accompanying drawings.

Brief Description of the Drawings

Figure 1 is a schematic block diagram showing a system embodying the present invention coupled to a software manufacturer's encryption apparatus;

Figure 2 is a flow diagram showing the steps involved in the preferred method of obtaining authorisation for installing a program, embodying the present invention; and

Figure 3 is a flow diagram showing several alternative steps involved in another method embodying the present invention.

Figure 4 is a flow diagram showing the sequence of events when running a program installed using the present invention.

Detailed Description of the Embodiments

Referring now to Figure 1, there is shown a system 1 embodying the present invention for preventing unauthorised installation of an application

program 2 on a computer. In this embodiment, the hardware used for the system 1 is that of a personal computer (PC). The system 1 comprises a CD-ROM optical reader device 3 for reading both the application program 2 and an authorisation set-up program 4 from a CD-ROM (not shown). If the application program 2 is supplied on the CD-ROM in compressed format, it is uncompressed during installation by the authorisation/set up program 4. The authorisation/set up program 4 includes a decryption key 5 which is described in detail hereinafter.

Both the application program 2 and the authorisation/set up program 4 are copied into a permanent data store (hard disk drive) 6 of the system 1. The data store 6 has an identification serial number 7 which is specific to this data store 6. The serial number 7 acts as the identifier code for the system 1. Typically, such serial numbers 7 are 32 bit numbers which can readily be accessed through the DOS command 'VOL', which displays the number 7 in Hexadecimal format as an eight digit number.

A microprocessor 8, connected to both the CD-reader 3 and the data store 6, is provided for controlling data flow and for effecting the authorisation procedure as will be described in detail hereinafter. In addition, the system 1 includes a display 9 for presenting messages to the user and a modem 10 for linking the system to a telecommunication network 11, in this case a telephone network.

The system 1 is connected via the telecommunications network 11 to the

software program manufacturer's or supplier's encryption device 12. The device 12 comprises a personal computer with a modem 13, a microprocessor 14 and a permanent hard disk drive 15. The hard disk drive 15 includes an authorisation program 16 which is used to encrypt data, using an encryption key 17, sent to the encryption device 12 by the system 1.

The first stage in the operation of the system 1 is to seek authorisation from the program manufacturer to install the program on the system 1. This process is carried out under the control of the system authorisation/set up program 4 and is described in detail hereinafter with reference to Figure 2.

The authorisation/set up program 4 is run at 20 and its first step is to read the hard disk serial number 7 at 21. It then requests the CD-ROM serial number from the user at 21A and the microprocessor 8 at 22 calls up the software manufacturer's encryption device 12 using the modem 10 to establish a communications link therewith. The manufacturer validates the CD-ROM serial number at 23, and if this is valid, the hard disk serial number 7 is sent to the encryption device 12 at 23A and is combined with the software identifier and the two codes are encrypted at 24 by the authorisation program 16 using the encryption key 17. The encrypted data (combined encrypted serial numbers) is then transmitted back to the system 1 at 25 via the already established communication link. The communications link between the system 1 and the encryption device 12 is then broken at 26.

The encrypted data is decrypted at 27 using the decryption key 5. The hardware identifier that results from the decryption step at 27 is compared at 28, 29 with the hard disk serial number 7 previously read at 21. If they correspond to each other, the use of the program 2 is authorised and the installation of the program 2 is allowed to proceed at 30. Installation usually involves expansion of the compressed program 2 to create relevant directories, pathways, readable files, executable files etc. If on the other hand, the serial number 7 and the decrypted data do not correspond, then use of the program is unauthorised and installation is prevented at 31. The user is notified at 32 of the unsuccessful installation by a message being put up on the display 9 and a warning against illegal copying of the program 2 is also displayed.

The present embodiment as described above uses a public/private cryptography technique, the general principles of which are well established and will not be described in great detail hereinafter. The reader is referred to "Cryptography: A New Dimension in Data Security" by Carl H. Meyer and Steven M. Matyas - John Wiley & Sons.

The public key is the decryption key 5 which is included in each copy of the program 2 that is sold. The private key is the encryption key 17 which is retained by the software manufacturer in the encryption device 12. The feature of public/private cryptography which makes it so useful is that knowledge of the public key does not enable the software hacker to compute the private key

without a great deal of effort. In addition, the public deciphering algorithm is different from the private enciphering algorithm and carries out steps in such a way as to not reveal the opposite steps required in the enciphering process. In this way, even though the software hacker has access to the decryption algorithm in the authorisation/set up program 4, he is not able to determine the encryption algorithm. In this embodiment, an RSA algorithm is used for the encryption/decryption processes. The RSA algorithm is described in detail in "Data & Computer Security" by Dennis Longley and Michael Shain, Macmillian Reference Books. This is particularly robust algorithm which is based on factorisation using large prime factors.

The comparison step 28, 29, as described above, requires the decryption result to correspond to the hard disk serial number 7. However, it is also possible for the decryption result and/or the hard disk serial number 7 to be further processed in a predetermined manner before this comparison is made. For example, the hard disk serial number may be exclusively read with a predetermined number prior to the comparison. This feature increases the resilience of this data protection system to software hackers.

In the embodiment described above the CD key is already written into the installation/set up program 4 and can be combined in a predetermined manner with the hardware serial number 7, for example by an Exclusive OR function, the result being transmitted to the encryption device 12. Various other ways can be

used to combine the CD key and the hard disk serial number 7 which all help to make the system more secure.

The above embodiment has been described using a telephone network 11. However, the present invention is not restricted to such a network which can be quite slow and has a restricted bandwidth. Rather, it is possible to use wide area networks (WANs) such as ISDN or dedicated internet connections which do not use the telephone network.

The process of obtaining authorisation as described in the above embodiment has been automatic without the need for human involvement. However, the invention is also applicable to software where the user does not have computer access or computer connection usually via a modem to a telecommunications network. In this situation, the authorisation/set up program 4 is modified as set out in Figure 3 where steps 23 to 27 of Figure 2 are replaced by corresponding steps 33 to 37.

Referring to Figure 3, the replacement step 33 to 37 are now described. The hard disk serial number 7 is presented at 33 to the user on the display 9. The CD-ROM serial number is presented at 33A to the user on the display 9 and the user then telephones the software manufacturer at 34 and communicates the hard disk serial number 7 and CD-ROM serial number to him (Step 34A). The software manufacturer encrypts at 35 the serial number 7 and the software identifier using the encrypting device 12 and the private encrypting key 17. The

manufacturer then communicates the encrypted combined code to the user at 36. Finally, the user enters the encrypted code into the system 1 at 37 which is used by the authorisation/set up program 4.

Figure 4 is a flow diagram illustrating the sequence of events which occur each time a software application installed on a computer using the present invention is run by the operator. In Figure 4, the loading of the installed application is initiated at 38 and as a first step 39 reads the hard disk serial number 7. This serial number is compared at 41,42 with the decrypted hard disk serial number read by the application at 40. If the two serial numbers correspond then the loading of the software application is allowed to continue at 43 and the loaded application may then be run by the operator. If, on the other hand, the two serial numbers do not correspond then the loading of the application ceases at 44 which may be followed by a warning notice to the operator at 45.

Various other modifications and improvements of the above described embodiments are possible without departing from the spirit and scope of the present invention as determined by the appended claims. For example, the encrypted hard disk serial number should be written directly into the main process of the authorisation/set up program 4, as it is being copied from the CD ROM or other medium to the hard disk 6 of the system 1. This makes subsequent dishonest modification and hacking more difficult. Other ways of improving the security of this system are set out below: Public and private keys should be

changed regularly, if possible for each new batch of CD-ROMs. Public and private keys can be different for each geographical region that the program 2 is sold in. The public key and associated variables should be directly coded into the main routine of the authorisation/set up program 4, as opposed to being parameters in the call to routines.

It should also be noted that the program does not have to be provided on CD-ROM. The invention is applicable to software provided on conventional floppy disks, by DVD's and to software delivered to the customer via a wide area network such as the internet or ISDN. Use of the invention in this latter case would mean that if software was illegally copied during transmission it would be unusable.

It is also to be appreciated that the present invention extends to any software program, even if installation of the program is not required. In this regard, use of the program even from CD-ROM, can be readily prevented by the present invention unless specific authorisation is obtained.

Although the description above refers to the communication of the computer serial number and software serial number to the software manufacturer or supplier it is to be understood that the communication can be to any remote location authorised by the software manufacturer at which registration and encryption can take place

CLAIMS:

1. A method for preventing unauthorised installation, copying or running of a computer program on a computer comprising the steps of:-

reading an identifier code associated with the computer;

encrypting the computer identifier code with a identifier code associated with the program;

tagging or marking the computer program with the encrypted combined identifier codes as it is installed from its storage medium onto the computer or is copied via the computer onto another or recipient medium;

decrypting the combined codes and comparing the decrypted tagged computer identifier code during running of the installed program, or during subsequent installation of the copied program, with the identifier code of the computer on which the program is installed or is being installed from the said recipient medium; and

preventing the running of the program or its installation if the second computer identifier code is not identical to or derivable in a pre-determined manner from the decrypted tagged identifier code.

2. A method according to claim 1, wherein the tagging is performed by a routine written into the computer program itself.

3. A method according to claim 1, wherein the tagging is performed by a routine written into the operating system of the computer.

4. A method according to claim 1, wherein the tagging is performed by a separately loaded security program.

5. A method according to any preceding claim, further comprising transmitting the computer identifier code and the program identifier code to a remote location for encryption with an encryption key.

6. A method according to claim 5, wherein said encryption key comprises a private key and said decryption key comprises a public key.

7. A method according to claim 5 or 6, wherein the encrypting and decrypting steps are carried out using an implementation of the RSA algorithm.

8. A method according to any one of claims 5 to 7, wherein the identifier codes are transmitted to the remote location and/or the encrypted identifier code data is received, via a telephone network.

9. A method according to any one of claims 5 to 8, wherein said transmitting

and/or receiving steps are carried out via the internet.

10. A method according to any of claims 5 to 8, wherein said identifier codes are transmitted to the remote location and/or the encrypted identifier code data is received, via a wide area network.

11. A method according to any of claims 1 to 10, further comprising displaying the hardware identifier code to the user after said reading step for subsequent encryption.

12. A method according to any preceding claim, further comprising displaying a message to the user when an attempted unauthorised installation or running of the program fails.

13. A method according to any preceding claim, wherein the computer identifier code is that of a permanent data store of the computer.

14. A method according to anyone of claims 1-13, wherein the identifier code is that of a PROM forming part of or associated with the CPU of the computer

15. A security system for preventing unauthorised installation of a program

in a computer or copying of a program by a computer, the system comprising:

means for reading the identifier code of the computer;

means for reading an identifier code of the program;

means for combining and encrypting the two identifier codes;

means for tagging or marking the program with the combined encrypted identifier codes during installation or copying;

means for decrypting the encrypted codes and comparing the decrypted tagged computer identifier code with the identifier code of the computer on which the program is run or being installed from a copy; and

means for preventing installation of said program if the decrypted tagged identifier code is not equivalent to or derivable from that of the computer on which the program is running.

16. A system according to claim 15 wherein the step of encryption comprise the use of a private key and step of decryption comprises the use of a public key.

17. A system according to claims 15 to 16 further comprising means for connecting said system to a telephone network for transmitting said identifier codes to said remote location and/or receiving the encrypted combined identifier code data.

18. A system according to claim 17 wherein said receiving and/or transmitting means are connected to the internet.

19. A system according to claim 16 further comprising

means for connecting said system to a wide area network for transmitting the identifier codes to the remote location and/or receiving the encrypted combined identifier code data.

20. A system according to any of claims 15 to 19, further comprising a display for displaying the identifier code for subsequent encryption and/or a message to the user when an attempted unauthorised installation of the program fails.

21. A system according to any of claims 15 to 20, wherein the identifier code is the identifier code of a permanent data store of the computer.

22. A system according to any of claims 15 to 20 wherein the identifier code is a serial number of a PROM forming part of or associated with the CPU of the computer.

23. A combination of a system according to any of claims 15 to 22, and an

encryption apparatus provided at a location remote from that of said system, the apparatus being arranged to encrypt the identifier codes using an encryption key.

24. A combination as claimed in claim 23, wherein the encryption apparatus further comprises means for receiving said identifier codes from said system and means for transmitting said encrypted combined identifier code data to said system.

25. A combination as claimed in claim 23 or claim 24 wherein the encryption apparatus uses public key/private key cryptography.

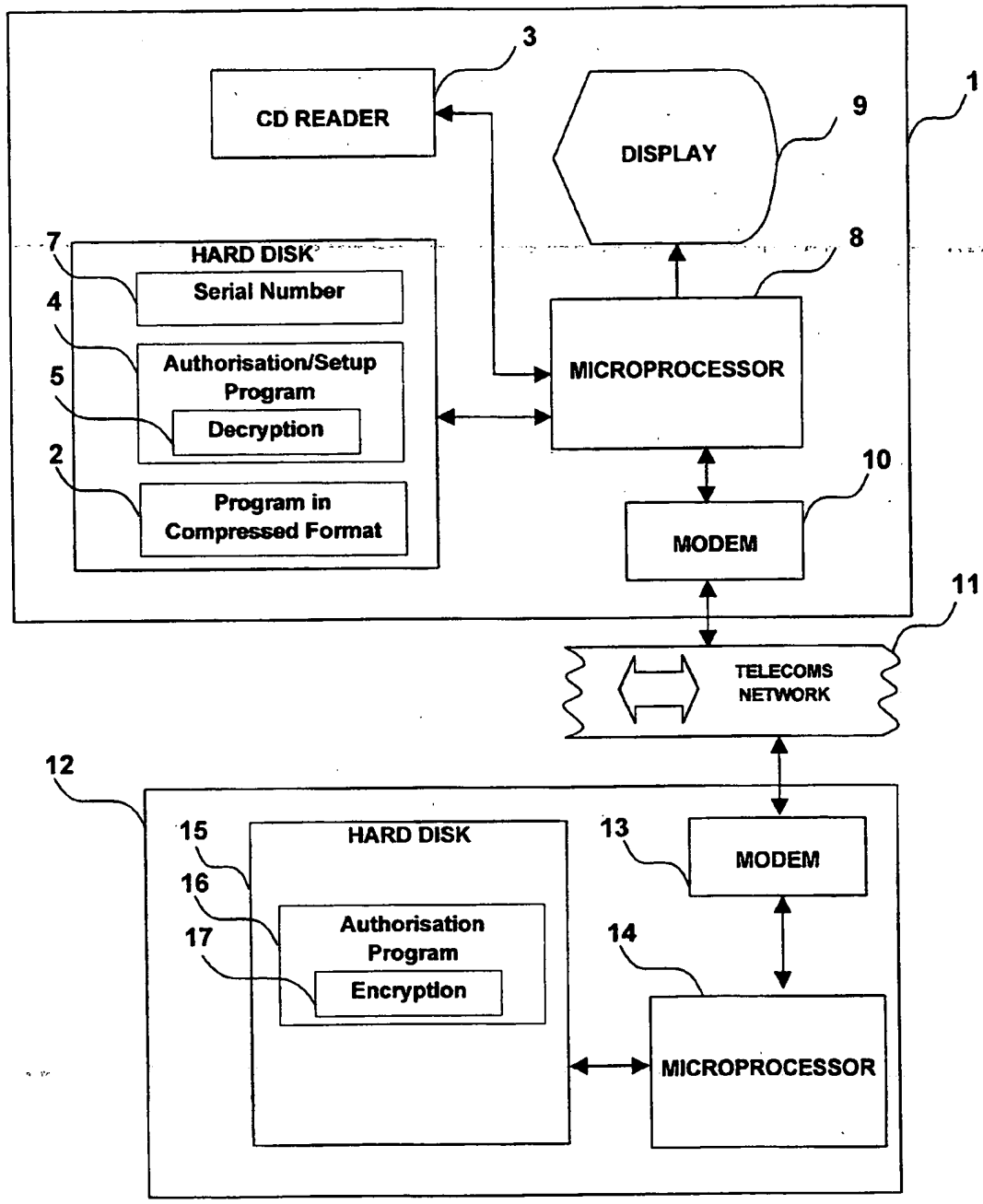

3
CD READER
1
9
DISPLAY
7
HARD DISK
8
Serial Number
4
Authorisation/Setup Program
MICROPROCESSOR
5
Decryption
2
Program in Compressed Format
10
MODEM
11
TELECOMS NETWORK
12
15
HARD DISK
13
MODEM
16
Authorisation Program
17
Encryption
14
MICROPROCESSOR

FIGURE 1

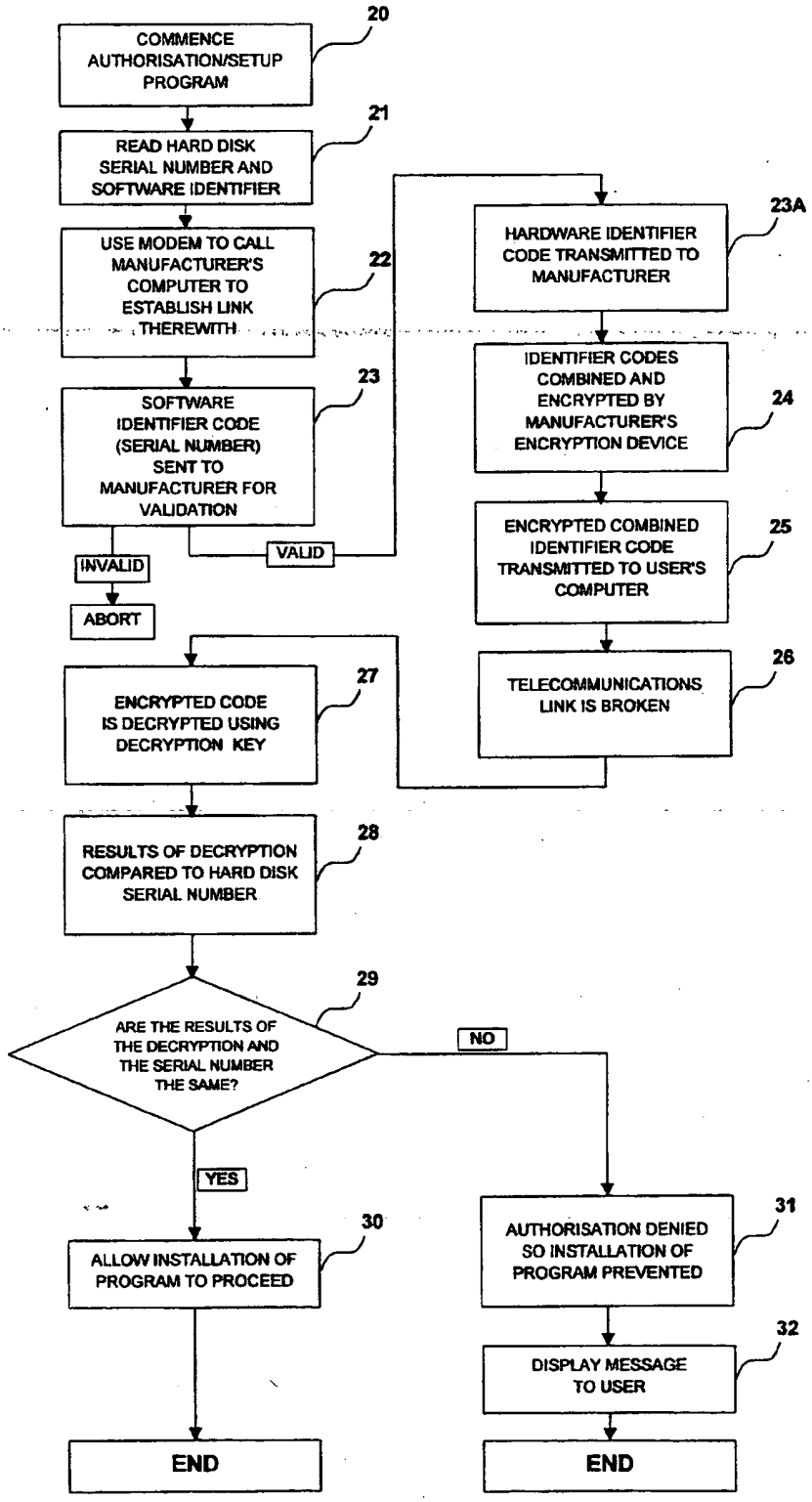


FIGURE 2

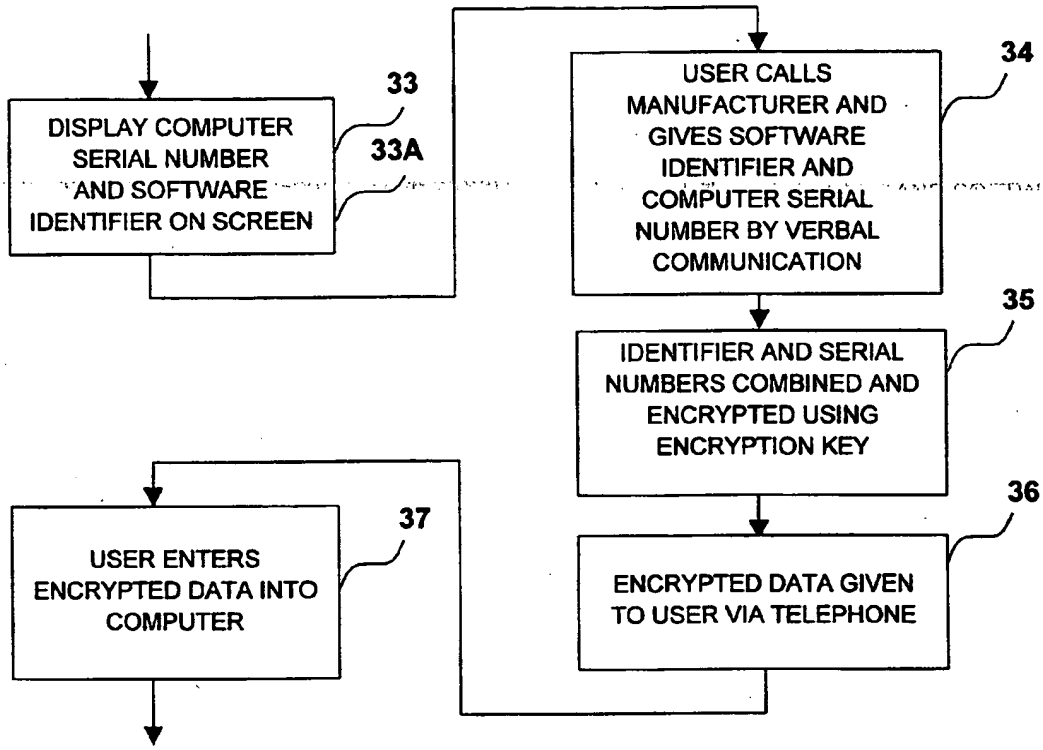

DISPLAY COMPUTER SERIAL NUMBER AND SOFTWARE IDENTIFIER ON SCREEN
33
33A
USER CALLS MANUFACTURER AND GIVES SOFTWARE IDENTIFIER AND COMPUTER SERIAL NUMBER BY VERBAL COMMUNICATION
34
IDENTIFIER AND SERIAL NUMBERS COMBINED AND ENCRYPTED USING ENCRYPTION KEY
35
ENCRYPTED DATA GIVEN TO USER VIA TELEPHONE
36
USER ENTERS ENCRYPTED DATA INTO COMPUTER
37

FIGURE 3

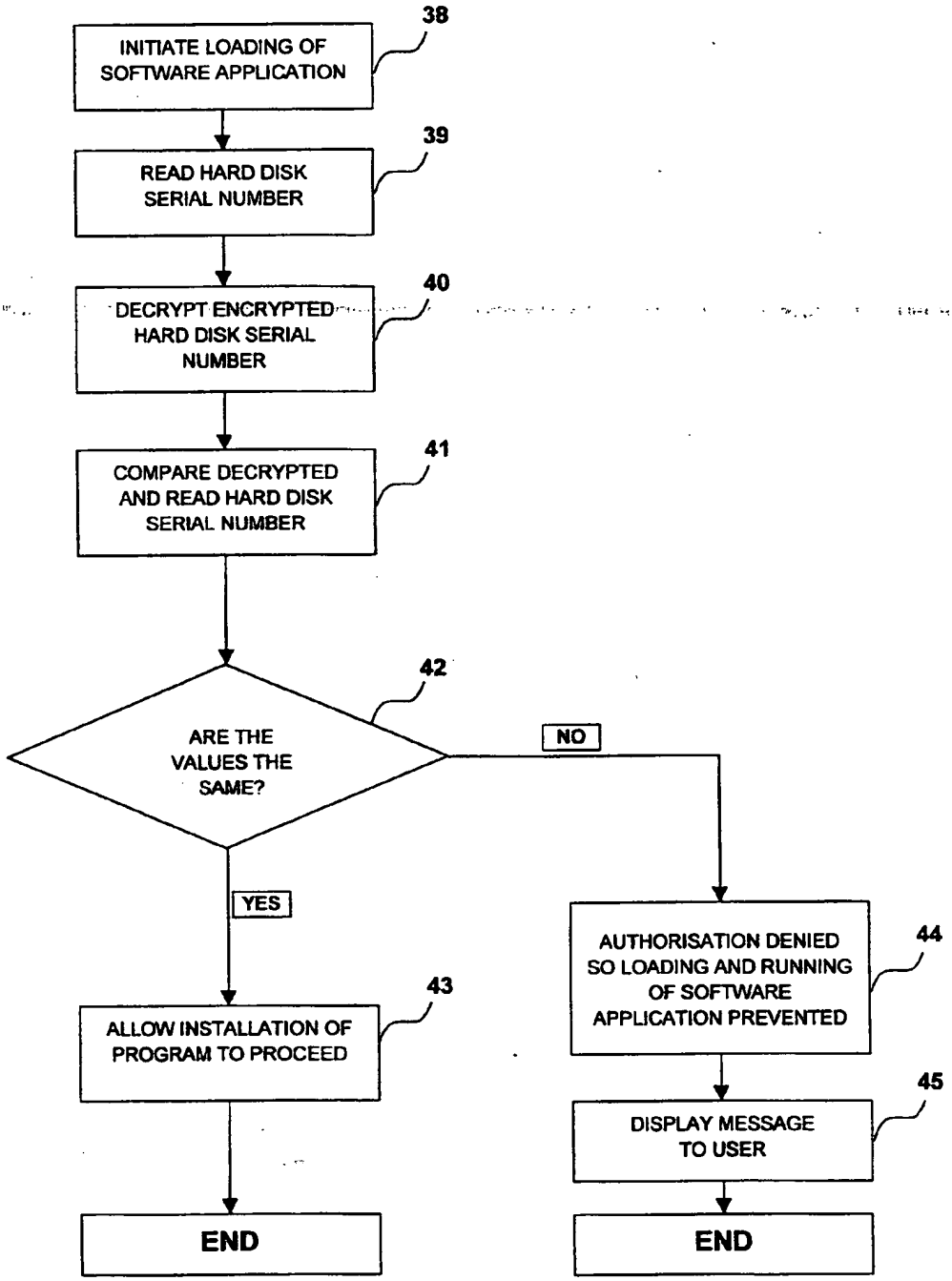

INITIATE LOADING OF SOFTWARE APPLICATION
38
READ HARD DISK SERIAL NUMBER
39
DECRYPT ENCRYPTED HARD DISK SERIAL NUMBER
40
COMPARE DECRYPTED AND READ HARD DISK SERIAL NUMBER
41
ARE THE VALUES THE SAME?
42
NO
YES
ALLOW INSTALLATION OF PROGRAM TO PROCEED
43
AUTHORISATION DENIED SO LOADING AND RUNNING OF SOFTWARE APPLICATION PREVENTED
44
DISPLAY MESSAGE TO USER
45
END
END

FIGURE 4

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/GB 98/03470

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 95 35533 A (MEGALODE CORP) 28 December 1995 see figures 4,5,15,16 see page 11, line 6 - page 16, line 22	1-6,8, 11-17, 20-25
A	US 5 113 518 A (DURST JR ROBERT T ET AL) 12 May 1992 see figures 1,2,4,13-16 see column 7, line 11 - column 11, line 8 see column 13, line 23 - column 14, line 38 see column 25, line 43 - column 32, line 32	1,4,5, 10-15, 20,21, 23,24

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 1999	18/02/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Inte ional Application No
PCT/GB 98/03470

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9535533 A	28-12-1995	AU 2666595 A	15-01-1996
US 5113518 A	12-05-1992	CA 1315001 A	23-03-1993
		GB 2219421 A,B	06-12-1989

Form PCT/ISA/210 (patent family annex) (July 1992)